Date of Approval: **January 18, 2022**

PIA ID Number: **6634**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Enterprise Telephone Database, ETD-1

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym, and milestone of the most recent PCLIA?

Enterprise Telephone Database, ETD-1 PCLIA #3692

What is the approval date of the most recent PCLIA?

2/19/2019

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

User and Network Services (UNS) Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e., system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The Enterprise Telephone Database (ETD-1) is a data warehouse, which stores information from various systems or sources (Aspect Automatic Call Distributors, Cisco, Intelligent Contact Management (ICM), AT&T Telephone Reports, Integrated Customer Contact Environment, Telephone Routing Information System Management Information System (MIS) regarding IRS telephone service to taxpayers. In addition to being the data repository for telephone MIS, ETD also contains custom-built reports/applications utilizing this telephone data. The ETD system summarizes the data and produces multiple web-based reports used to evaluate the effectiveness of Internal Revenue Service telephone operations to properly evaluate the prior day's telephone performance. In addition to the web-based reports, ETD has a partitioned file share area which contains data from queries which are run against the ETD databases. It allows Joint Operations Center (JOC) and Business Operating Division (BOD) analysts to use the data to analyze call patterns/activity related to their program areas. The primary users are JOC personnel, Wage & Investment and Small Business Self Employed BOD analysts both Compliance and Accounts Management; Tax Exempt Government Entities analysts, and managers at each of the IRS call sites.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e., last 4 digits, etc.)?

No

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?

Yes

Specify the PII Elements:

Phone Numbers
Standard Employee Identifier (SEID)

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant).

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

PII for personnel administration is 5 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The collection and display of taxpayer's Automatic Number Identification (ANI) allows the IRS to understand, interpret and diagnose taxpayer service issues to improve quality. This information will identify congestion and demand against IRS toll free products that may subsequently require redesign or additional staffing to reduce the number of dialed attempts required to receive service. Organizations may request this information, but special independent queries must be run against call detail records to cull and produce this information. In addition to the ANI, call detail records include information about the agent that answered the call Standard Employee Identifier (SEID) how and/or why a call was disconnected or abandoned, date/time of the call, original Customer Dial Number, information on call duration, such as talk time, hold time, warp time, queue time, router call key/unique identifier for the call, skill group that handled the call, application the call was sent to (i.e. Refunds, Individual Master File Accounts), which sites were available for queueing the call, language the customer selected, and announcements that played throughout the call.

How is the SBU/PII verified for accuracy, timeliness, and completion?

The ETD reports are not driven by SBU/PII data, but by the information pertaining to the telephone call that is contained in the call detail records. The information is received directly from the Enterprise Telephone Database. The system/database/application is deemed reliable and accurate. The information is not altered in any way. There is no validation of SBU or PII data because there is no report created in ETD that contains that type of data. Part of the call record is the customer's telephone number and the SEID of the assistor that handled the call. Telephone data is downloaded from Verizon telephone databases and compiled into a readable report. That data is then compared to prior week and year data along with other analyses to verify accuracy and completeness.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 34.037 Audit Trail and Security Records

IRS 00.001 Correspondence Files and Correspondence Control Files

IRS 36.003 General Personnel and Payroll Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Aspect Automated Call Distributors
Current PCLIA: No
SA&A: No

System Name: Intelligent Contact Manager
Current PCLIA: No
SA&A: No

System Name: Unified Contact Center Enterprise
Current PCLIA: No
SA&A: No

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

No

Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

The only PII collected into the system is the phone number provided in the reports received from Verizon and the employee's SEID from ICM. Neither the phone number nor the SEID information is used in any reports in the system.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

The phone number is captured when the individual calls the IRS Toll Free number and there is not an option for the customer to not provide a phone number. The information is collected while carrying out the Internal Revenue laws of the United States; an individual cannot decline providing the information. The SEID is needed to determine if a call was answered by an assistor but is not displayed in any of the performance reports.

How does the system or business process ensure 'due process' regarding information access, correction, and redress?

This system primary function is to provide performance measures on IRS Telephone Operations. Customer phone numbers plays no part in performance reporting. The system does not replace any individual taxpayer's right to due process, as dictated by the Internal Revenue Manual guidelines. IRS policy allows individual taxpayers whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. However, due to the nature of this system, individuals may not receive specific notice that their information has been collected.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and operated; IRS owned, contractor operated; contractor owned and operated).

IRS Owned and Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Read Write

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Read Only

Contractor Developers: Read Only

How is access to SBU/PII determined and by whom?

Access to the raw data is approved by the project manager based solely upon impact to the system performance. This is the only method the PII in the system can be accessed and is not available to the average user. Access to the information is only granted through either the OL5081 or Business Entitlement Access Request System (BEARS) application. The ETD SYS ADMIN (Enterprise Telephone Database) system utilizes the standard IRS on-Line access application to document approvals for access. Data access is granted on a need-to-know basis. Access approval is based on the Users role(s) and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments; they are restricted from changing the boundaries of their access without management approval. The Enterprise Telephone Database system utilizes the standard IRS on-Line access application to document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access to their local management for approval. Users are not permitted access without a signed form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. The employee's access will be terminated once they no longer require access to the Database. Deletion from the active access role is also performed through the OL5081.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

The IRS Identity and Records Protection Office is currently developing a new section under Records Control Schedule specific to ETD and electronic records retention. GRS 5.2 Item 020-Intermediary records. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

No audit trail, for users of the ETD-1 website, has been implemented because there was no benefit in tracking detailed user information when the data available to the user in EDT-1 could not be used to identify an individual and all users were behind the IRS firewall. Access to the database is controlled by the OL5081 process. In addition, any change to production coming out of the development/test environments are submitted via the transmittal process. The transmittal contains the developer's name and phone number. Further, only the System Analysts (the specific IRS Information Technology employees) have "write" access. This small group of IRS employees as well as all other users of the database would have to use Microsoft Sequel (SQL) queries to see EDT-1 data and the SQL logs are the audit trail for those actions. Their access is also obtained through the OL5081 application. SQL logging functionality is currently unavailable to us due to space limitations on the production server. To ensure the auditability of the ETD-1 system, a custom audit trace has been installed as part of IRS database hardening. Audit logs are written to a file and stored on the P: Drive for all ETD-1 SQL servers. All events are audited. In addition to the custom audit trace, the Default Trace is enabled for all ETD-1 SQL servers, which captures database events, errors and warnings, full-text events, object events, security audit events, configuration changes and server memory events. ETD-1 web server (IIS) session events/requests are tracked in a separate log for each website instance, e.g., ETD, Organization Function and Program Codes, etc. on all ETD-1 IIS servers.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

All monitoring and evaluating activities are done by the ETD-1 programs that manage the ETD-1.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax, or Privacy Act consent?

Yes

Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.

Yes